REMARKS

The application has been amended in a manner believed to place it in condition for allowance at the time of the next Official Action.

Amendments to the Disclosure

Independent claim 10, dependent claims 14-19, independent claim 20, dependent claims 21-22, independent claim 24, and dependent claim 25 are amended to recite the invention based on PCT/JP2005/001524.

The claims are further amended as to style in consideration of U.S. practice and preferences. The amendments to the claims are not believed to introduce new matter.

Independent claim 10, dependent claims 11-12, independent claim 13, dependent claims 14-19, independent claim 20, dependent claims 21-22, independent claim 24, and dependent claim 25, remain pending.

Dependent claims 23 and 26 have been canceled without prejudice.

Formal Matters - Objections to the Claims

The Official Action objected to claim 10, stating that the phrase “either of” needs to be changed to “one of” because the claim language provides more than two alternative conditions.

In response, claim 10 is amended in a manner believed to overcome the Official Action's objection. Withdrawal of the objection to the claims is thereby respectfully requested.

Rejection of claims 10-12, 15-17, 20-23 under Section 103

Claims 10-12, 15-17 and 20-23 were rejected under 35 U.S.C. §103(a) as being unpatentable over Chesla (US 2004/0250124; hereinafter CHESLA) in view of Chao et al. (US 7,526,807; hereinafter CHAO). This rejection is respectfully traversed for the reasons below.

CHESLA discloses a method for detecting an attack using a number of occurrences of the packets characterized by one of the plurality of parameters, whereas independent claims 10 and 20 are directed to judge an unauthorized attack based on "the number of distinct values" observed in the pre-specified fields in the packet header. That is, one of the judgment indicators of independent claims 10 and 20 is "the number of distinct values", (for example "the number of distinct values" of source address field, or port number field, or destination address field, etc.); this is not disclosed in CHESLA.

For example, in a case where distinct source addresses S_1, S_2, $\cdots$,S_N are observed in the source address field of the M packets ($M \geq N$) seen within a pre-specified time interval, "the number of distinct values" is N. In a case where "the number of

distinct values" of source address field increases, it is judged that an unauthorized attack (for example, a DDos attack) may be in progress.

CHAO discloses determining packets to be described in response to a DDos attack using the equation that is computed by comparing currently measured attribute values to nominal attribute values, and using various thresholds and combinations thereof. In contrast, independent claims 10 and 20 are directed to judge an unauthorized attack by computing the ratio of "the number of distinct values" to other numbers (described in conditions (a)-(d)) and determining whether the ratio reaches the pre-specified threshold. That is, the judgment point of independent claims 10 and 20 is to use the ratio of "the number of distinct values" to other numbers instead of the number of values, and this is disclosed in CHAO.

For example, in a case where the number of packets and "the number of distinct values" of source address field are observed within a pre-specified time interval (e.g., 16:00-16:30 as shown in the chart presented below), it is judged that an unauthorized attack (for example, a DDos attack) may be in progress within the time 16:20-16:25 because the ratio of "the number of distinct values" to number of packets has been seen to increase within the time 16:20-16:25.

Time	The number of packets	The number of distinct values
16:00-16:05	3,500	20
16:05-16:10	5,000	25
16:10-16:15	65,000	325
16:15-16:20	7,500	40
16:20-16:25	4,000	170
16:25-16:30	4,500	22

Therefore, the accuracy of detecting an unauthorized attack will be increased independently of the increase and/or decrease of the number of packets due to using the ratio of "the number of distinct values" to other numbers. Thus, this will avoid a faulty judgment in case the traffic fluctuates widely and randomly in a network with a WEB server.

As clarified above, independent claims 10 and 20 have a remarkable effect not present in CHESLA's disclosure and CHAO's disclosure, and it would not have been obvious to a person having ordinary skill in the art at the time the invention was made to modify CHESLA and incorporate CHAO to meet the preceding limitations.

Dependent claims 11 and 21 are directed to judge an unauthorized attack based on "the number of distinct values" observed in the arbitrary combinations of two or more fields in the packet header; this also is not disclosed in CHESLA and CHAO.

For example, in a case where "the number of distinct values" of source address field and port number field are observed, an unauthorized attack will be judged according to the

application classification. Thus, an unauthorized attack such as a minor DDos attack with few changes in the number of addresses will be detected independently of the increase and/or decrease in the number of packets.

Dependent claim 11 in combination with independent claim 10 and dependent claim 21 in combination with independent claim 20 have a remarkable effect of increasing the accuracy of detecting an unauthorized attack. This effect does not exist in either of CHESLA's disclosure or CHAO's disclosure.

Dependent claims 12 and 22 are directed to judge an unauthorized attack based on the TTL value in addition to "the number of distinct values" observed in the packet header fields; this also is not disclosed in CHESLA and CHAO. Dependent claim 12 in combination with independent claim 10 and dependent claim 22 in combination with independent claim 20 have a remarkable effect of increasing the accuracy of detecting an unauthorized attack. This effect does not exist in either of CHESLA's disclosure or CHAO's disclosure.

Dependent claim 15 is directed to determine the source address of an unauthorized attack by using the network attack detection system described in claim 10; this also is not disclosed in CHESLA and CHAO. Dependent claim 15 in combination with independent claim 10 has a remarkable effect of increasing the accuracy of searching the source address of an unauthorized

attack. This effect does not exist in either of CHESLA's disclosure or CHAO's disclosure.

Dependent claim 16 is directed to locate the source address of an unauthorized attack by using the network attack detection system described in claim 11; this also is not disclosed in CHESLA and CHAO. Dependent claim 16 in combination with independent claim 11 has a remarkable effect of increasing the accuracy of searching a source address of an unauthorized attack. This effect does not exist in either of CHESLA's disclosure or CHAO's disclosure.

Dependent claim 17 is directed to search a source address of an unauthorized attack by using the network attack detection system described in claim 12; this also is not disclosed in CHESLA and CHAO. Dependent claim 17 in combination with independent claim 12 has a remarkable effect of increasing the accuracy of searching a source address of an unauthorized attack. This effect does not exist in either of CHESLA's disclosure or CHAO's disclosure.

It is therefore respectfully submitted, for at least the reasons foregoing, that claims 10-12, 15-17 and 20-23 are non-obvious over CHESLA in view of CHAO. Withdrawal of the rejection of claims 10-12, 15-17 and 20-23 under Section 103 is thereby respectfully requested.

Rejection of claims 13-14 and 24-25 under Section 102

Claims 13-14 and 24-25 were rejected under 35 U.S.C. §102(e) as being unpatentable over CHESLA. This rejection is respectfully traversed for the reasons below.

CHESLA discloses a method for detecting an attack using a number of occurrences of the packets characterized by the one of the plurality of parameters, whereas independent claims 13 and 24 are directed to judge an unauthorized attack based on "the number of distinct values" observed in the arbitrary combinations of two or more fields in the packet header. That is, one of the judgment indicators of independent claims 13 and 24 is "the number of distinct values" (for example "the number of distinct values" of source address field, or port number field, or destination address field, etc.); this is not disclosed in CHESLA.

For example, in a case where distinct source address S_1, S_2, $\cdots$,S_N are observed in the source address field of the M packets ($M \geq N$) seen within a pre-specified time interval, "the number of distinct values" is N. For example, in a case where "the number of distinct values" of source address field and port number field are observed, an unauthorized attack will be judged according to application classification. Thus, an unauthorized attack such as a minor DDos attack with few changes in the

number of addresses will be detected independent of the increase and/or decrease in the number of packets.

Further, dependent claims 14 and 25 are directed to judge an unauthorized attack based on the TTL value in addition to "the number of distinct values" observed in the packet header fields; this feature is not disclosed CHESLA and further is not disclosed in CHAO. Dependent claim 14 in combination with independent claim 13 and dependent claim 25 in combination with independent claim 24 have a remarkable effect of increasing the accuracy of detecting an unauthorized attack. This effect does not exist in CHESLA's disclosure, and further does not exist in CHAO's disclosure.

It is therefore respectfully submitted that claims 13-14 and 24-25 are not anticipated by CHESLA, and further the features recited in claims 13-14 and 24-25 are not anticipated by either of CHESLA or CHAO, individually or in combination. Withdrawal of the rejection of claims 13-14 and 24-25 under Section 102 is thereby respectfully requested.

Rejection of claims 18-19 and 26 under Section 103

Claims 18-19 and 26 were rejected under 35 U.S.C. §103(a) as being unpatentable over CHESLA as applied to claims 13, 14 and 24 above and further in view of CHAO. This rejection is respectfully traversed for the reasons below.

Dependent claim 18 is directed to locate the source address of an unauthorized attack by using the network attack detection system described in claim 13, and this is not disclosed in CHESLA and CHAO. Dependent claim 18 in combination with independent claim 13 has a remarkable effect of increasing the accuracy of searching a source address of an unauthorized attack. This effect does not exist in CHESLA's disclosure and CHAO's disclosure.

Dependent claim 19 is directed to locate the source address of an unauthorized attack by using the network attack detection system described in claim 14, and this is not disclosed in CHESLA and CHAO. Dependent claim 19 in combination with independent claim 14 has a remarkable effect of increasing the accuracy of searching a source address of an unauthorized attack. This effect does not exist in CHESLA's disclosure and CHAO's disclosure.

For at least the reasons presented above, it is respectfully submitted that claims 18-19 and 26 are non-obvious over CHESLA in view of CHAO. Withdrawal of the rejection of claims 18-19 and 26 under Section 103 is thereby respectfully requested.

Conclusion

From the foregoing, it will be apparent that Applicant has fully responded to the July 6, 2010 Official Action and that

the claims as presented are patentable. In view of this, Applicant respectfully requests reconsideration of the claims, as presented, and their early passage to issue.

In order to expedite the prosecution of this case, the Examiner is invited to telephone the attorney for Applicant at the number provided below if the Examiner is of the opinion that further discussion of this case would be helpful in advancing prosecution.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON

/Jeremy G. Mereness/

Jeremy G. Mereness, Reg. No. 63,422
209 Madison Street
Suite 500
Alexandria, VA 22314
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

JGM/lrs